Commun Nonlinear Sci Numer Simulat 62 (2018) 395–408

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

Research paper

Digitally generating true orbits of binary shift chaotic maps and their conjugates

İsmail Öztürk[a,*], Recai Kılıç[b]

[a] Department of Electrical & Electronics Engineering, Amasya University, Merkez, Amasya 05100, Turkey
[b] Department of Electrical & Electronics Engineering, Erciyes University, Melikgazi, Kayseri 38039, Turkey

ARTICLE INFO

Article history:
Received 18 May 2017
Revised 13 September 2017
Accepted 25 February 2018
Available online 2 March 2018

Keywords:
Dynamical maps
True chaotic orbits
FPGA
Topological conjugacy

ABSTRACT

It is impossible to obtain chaotic behavior using conventional finite precision calculations on a digital platform. All such realizations are eventually periodic. Also, digital calculations of the periodic orbits are often erroneous due to round-off and truncation errors. Because of these errors, periodic orbits quickly diverge from the true orbit and they end up into one of the few cycles that occur for almost all initial conditions. Hence, digital calculations of chaotic systems do not represent the true orbits of the mathematically defined original system. This discrepancy becomes evident in the simulations of the binary shift chaotic maps like Bernoulli map or tent map. Although these systems are perfectly well defined chaotic systems, their digital realizations always converge to zero. In the literature, there are some studies which replace the least significant zero bits by random bits to overcome this problem.

In this paper, we propose the algorithms using this simple method for digitally implementing binary shift chaotic maps. These algorithms are suitable for both software and hardware solutions, and they are also applicable with any random number generator or a repeated bit sequence. According to the type of the random number generator, either true periodic orbits or true chaotic orbits of the map are obtained. Moreover, it is shown that, utilizing topological conjugacies, obtained true orbits of binary shift chaotic maps can be used to calculate true orbits of other maps such as logistic and Chebyshev maps which are normally subject to round-off and truncation errors. The hardware implementations of binary shift chaotic maps, logistic map and Chebyshev maps have been realized on a Field Programmable Gate Array (FPGA) platform using the proposed algorithms.

1. Introduction

Many papers about chaos-based cryptography are published each year. These papers often propose a cryptography scheme depending on digital implementations of chaotic systems, and mostly the chosen system is a discrete-time map [1–7]. The general motivation for using chaotic systems as part of a cryptography scheme is due to the closeness between the properties of chaos and the requirements of cryptography [8]. These properties of chaos are expressed as follows: (i) mixing; (ii) sensitive dependence on initial conditions; (iii) random-like behavior [9–12]. However, it is well-known but mostly neglected that digital implementations of chaotic systems can only produce periodic orbits due to finite precision

* Corresponding author.
E-mail address: ismail.ozturk@amasya.edu.tr (İ. Öztürk).

https://doi.org/10.1016/j.cnsns.2018.02.039
1007-5704/

and they produce short cycles due to round-off and truncation errors [13,14]. Some solutions have been proposed to overcome this problem [15]. But it is shown in [14] that after some transients almost all of the initial conditions fall into one of the few cycles due to transient and cycle intersections. The same study reveals that cycles with the same lengths are identical (circularly shifted versions of each other). Therefore, trying to increase cycle lengths is not useful for chaos-based cryptography. Instead, the perturbation method proposed in [16] can be applied within short time intervals to avoid an orbit to fall into one of the mentioned cycles.

Even though this short cycle problem is solved by some method, we can't assume that the properties of chaos described above are preserved. First of all, the sensitivity on initial conditions property is not the same with what is originally meant. In chaotic systems, two arbitrarily close orbits are guaranteed to be within a specific distance after some iterations. This property is demonstrated on computers by choosing two nearby initial conditions and observing their divergence. However, due to mixing (or under weaker assumption topological transitivity) and boundedness, these orbits may become arbitrarily close to each other once again, but they do not intersect due to the same property. On the contrary, they may (and most likely) intersect in digital realizations, so the sensitive dependence property collapses after some point [14]. Obviously, such a behavior cannot be considered as a strong random-like behavior.

For these reasons, digital implementations of chaos are not the same with their original mathematical constructions. This should be evident considering their domains. While the original models are defined on a continuum which contains uncountably many numbers, the numbers available on a digital platform are discrete and finite. This is a problem even for choosing the initial condition. When we try to calculate the orbit of the initial condition $\pi/4$ of some map digitally, we actually choose an initial condition which is close to $\pi/4$. We can't choose the exact initial condition because it is an irrational number and it cannot be expressed exactly. Although, choosing nearby numbers does not pose a significant problem for many other engineering applications, choosing even a slightly different number yields a completely different orbit in a chaotic system. Therefore, we can't even begin to calculate the true chaotic orbits of many (in fact, uncountably many) numbers. Even if the chosen initial condition can be completely expressed on a digital platform, there is no guarantee that other points in the orbit can be expressed exactly.

Above arguments should make it clear that the orbits obtained on a digital platform using the conventional fixed or floating point computations are not the true orbits of the original model. This discrepancy has drastic consequences for the digital realizations of the maps like Bernoulli map, tent map, and Baker's map. All simulations of these maps converge to zero regardless of the chosen initial condition [17]. The common property of these maps is their parameter values. All of their multiplication parameters are powers of two and they don't have any arithmetic operations that cause round-off or truncation. Since multiplications by powers of two can be performed as binary shifts, we will call such maps "binary shift chaotic maps". These maps converge to zero on digital platforms, because numbers are expressed by a finite number of bits and left shift operations force least significant bits to be zero. After some iterations these zeros fill the whole memory storage unit, and hence, the orbit converges to zero.

To overcome this problem, in many studies the original map is modified [18–22]. In other studies, parameter values are chosen very close to the power of two or a different parameter value is chosen [23–27]. In both cases, the shift operations are avoided and round-off and truncation errors are induced along the computations. The resulting orbits for such cases are the deficient (or pseudo) orbits mentioned above.

However, since binary shift chaotic maps are free from round-off or truncation errors, they are the natural candidates for computing the true periodic or chaotic orbits of a chaotic system. Therefore, the studies about digital calculations of true chaotic orbits usually revolve around binary shift chaotic maps. In [28], it is argued that true chaotic orbits of Bernoulli map can be calculated by choosing computable numbers as initial conditions [29]. However, every computable initial condition like π or e requires an algorithm (like the one in [30]) for computation and this means that every initial condition should have a different implementation. Also, computations may get complicated as the digits of the initial condition are computed while the accuracy of the computations decays. For these reasons, this method is more convenient for producing true chaotic orbits for specific initial conditions up to N iterations while N depends on the algorithm.

In a recent study, a method is proposed for digitally calculating true orbits of 1-dimensional piecewise-linear chaotic maps which can be expressed as linear fractional maps [31]. True chaotic orbits of the Bernoulli map are calculated for a limited number of iterations in this study. But the proposed method relies on integer calculations of the coefficients of cubic polynomials and the coefficients of these polynomials become huge as the iterations increase. Hence, calculations become impractical very quickly. Also, the calculation of the values of the points in the orbit requires solving the roots of cubic polynomials each iteration, and this process is not favorable for hardware implementations. It should be noted that, in this method, the initial conditions are represented by algebraic numbers but almost all of the real numbers are transcendental numbers [32].

Since these methods are not as easy as simply applying conventional fixed or floating point calculations, there are not many papers about true orbit generations and papers about applications of chaos mostly do not make a distinction between true chaos and its digital implementations as we have stated above [1–6]. In order to clear the misconceptions about the digital implementations of chaos in the literature, simpler methods are needed for true orbit generation. A simpler and straightforward approach for generating true orbits is to replace the least significant zero bits (LSB) by random or repeated bit patterns. There are a few studies which apply this idea in the literature [33–35]. In [33,34] register part of a shift register is treated as the approximation of the Bernoulli map and least significant bit of the shift register is replaced by a i.i.d (independent and identically disturbed) bit sequence to produce true periodic orbits of the Bernoulli map. Additionally,